

“Everything you ever wanted to know about PCI Compliance but were afraid to ask”

Brought to you by

SOLVERAS
PAYMENT SOLUTIONS™

1. What is the PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment. This covers essentially any merchant that has a Merchant ID (MID).

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006, to manage the ongoing evolution of the PCI security standards, with a focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB). The Standards can be found on the PCI SSC's Web site: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

2. How is “cardholder data” defined?

Cardholder data is the full magnetic stripe or the Primary Account Number plus any of the following:

- Cardholder Name
- Expiration Date
- Service/CVV Code

3. To whom does the PCI DSS apply?

PCI applies to ALL organizations or merchants (regardless of size or number of transactions), which accept, transmit or store any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

4. What are the PCI Compliance deadlines?

All merchants that store, process or transmit cardholder data must be compliant now. However, as a Level 4 merchant (< 20,000 credit card transactions/year), you will have to refer to your processor for their specific validation requirements. All deadline enforcement will come from your processor. You may also find more information on Visa's Web site: http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf.

5. How long will this take?

The length of the process varies. Once non-compliance issues have been identified, the amount of time it takes an organization to implement solutions will affect the length of the process. The amount of time involved also varies depending on the complexity of the environment.

6. What is the PCI Self-Assessment Questionnaire?

The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the PCI DSS. In February 2008, the PCI SSC released four versions of the questionnaire to account for different business environments.

1. SAQ A: Addresses requirements applicable to businesses that have outsourced all cardholder data storage, processing and transmission.
2. SAQ B: Created to address requirements pertinent to businesses that process cardholder data via imprint machines or standalone dial-up terminals only.
3. SAQ C: Constructed to focus on requirements applicable to businesses whose payment application systems are connected to the Internet.
4. SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ, and those merchants who do not fall under the types addressed by SAQ A, B or C.

7. I'm a small merchant who has limited payment card transaction volume. Do I need to be compliant with PCI DSS?

All merchants, whether small or large, need to be PCI compliant. The payment brands have collectively adopted PCI DSS as the requirement for organizations that process, store or transmit payment cardholder data. PCI SSC is responsible for managing the security standards while each individual payment brand is responsible for managing and enforcing compliance to these standards.

8. What are the requirements for PCI DSS Compliance?

There are 12 requirements that fall into six categories:

1. Build and Maintain a Secure Network: Install and maintain a firewall, and use unique, high-security passwords, with special care to replace default passwords.
2. Protect Cardholder Data: Whenever possible, do not store cardholder data. You must also encrypt any data passed across public networks, including your shopping cart and Web-hosting providers.
3. Maintain a Vulnerability Management Program: Use anti-virus and keep it up-to-date. Develop and maintain secure operating systems and payment applications. Ensure the applications you use are compliant (see www.visa.com/pabp).
4. Implement Strong Access Control Measures: Access — both electronic and physical — to cardholder data should be on a “need-to-know” basis. Ensure those people with access have a unique ID and password. Do not share log on information.
5. Regularly Monitor and Test Networks: Track and monitor all access to networks and cardholder data. Ensure you have a regular testing schedule for security systems and processes: firewalls, patches and anti-virus.
6. Maintain an Information Security Policy: It's critical that your organization has a resource for how data security is handled at your business. Ensure you have a policy and that it's disseminated and updated regularly.

9. What is a Network Vulnerability Scan?

A network vulnerability scan is an automated, non-intrusive scan that assesses your network and Web applications from the Internet (on the external-facing IPs). The scan will identify any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to your network and potentially compromise cardholder data. The scans provided will not require you to install any software on their systems, and no denial-of-service attacks will be performed.

10. What if my business does not go through this compliance procedure?

If you do not comply with the security requirements of the card associations, you put your organization at risk of payment card compromise. Your acquirer may also pass fines (levied by the card associations for non-compliance) on to you.